$$341 = (21-10)(21+10)$$

$$341 = 11 \cdot 31$$

حسب فيرما بما أن 2 أولي مع 11

$$2^{10} \equiv 1 \pmod{11}$$

ومنه

$$2^{31} = (2^{10})^3 \cdot 2 \equiv 2 \pmod{11}$$

ملاحظة ثانية

$$2^{11} \equiv (2^5)^2 \cdot 2 \pmod{31}$$

$$2^{11} \equiv (32)^2 \cdot 2 \pmod{31}$$

$$\equiv (1)^2 \cdot 2 \pmod{31}$$

$$2^{11} \equiv 2 \pmod{31}$$

حسب المثال السابق

$$2^{31 \cdot 11} \equiv 2 \pmod{31 \cdot 11}$$

$$2^{341} \equiv 2 \pmod{341}$$

$$2^{340} \cdot 2 \equiv 2 \pmod{341}$$

بما أن 2 أولي مع القاسم أي 2 أولي مع 341 وبالتالي يمكن الاختصار من طرفي التطابق.

$$2^{340} \equiv 1 \pmod{341}$$

ط) بما أن 2 و 11 أوليان فيما بينهما

$$2^{10} \equiv 1 \pmod{11}$$

$$(2^{10})^{34} \equiv 1 \pmod{11}$$

$$2^{340} \equiv 1 \pmod{11}$$

$\Rightarrow 11 \mid (2^{340} - 1)$

صفحة ثانية

حيا أن 2 و 31 أوليان فيما بينهما

$2^{30} \equiv 1 \pmod{31}$

$2^{340} = (2^{30})^{11} \cdot 2^{10} \equiv 2^{10} \pmod{31}$

$\equiv (2^5)^2 \pmod{31} \equiv 1 \pmod{31}$

$2^{340} \equiv 1 \pmod{31}$

$\Rightarrow 31 \mid (2^{340} - 1)$

ولأن 11 و 31 أوليان فيما بينهما وبالتالي فإن

$31 \cdot 11 \mid (2^{340} - 1)$

$\Rightarrow 341 \mid (2^{340} - 1) \Rightarrow$

$2^{340} \equiv 1 \pmod{341}$

هذا المثال يبين أن عكس مبرهنة فرما ليس صحيحاً في الحالة العامة

$2^{340} \equiv 1 \pmod{341}$

341 ليس أولياً

* أي إذا كان

$a^{m-1} \equiv 1 \pmod{m}$

وبالتالي ليس بالضرورة أن يكون m أولياً

/ /

* الأعداد من النوع

$$2^n \equiv 2 \pmod{n}$$

تسمى أشباه أولية وهي مجموعة غير منتهية

تمرين: سؤال امتحان

بين أنه إذا كان $d(a,35)=1$ ، $d(a,5)=d(a,7)=1$

فأثبت أن

$$a^{12} \equiv 1 \pmod{35}$$

$$a^{4} \equiv 1 \pmod{5} \Rightarrow a^{12} \equiv 1 \pmod{5}$$

$$a^{6} \equiv 1 \pmod{7} \Rightarrow a^{12} \equiv 1 \pmod{7}$$

5 ، 7 أولية متباينة وبالتالي هذا يتم نعم 12

إذا كان $d(a.b,42)=1$ فأثبت أن

$$(a^6 - b^6) \equiv 0 \pmod{168}$$

$$168 = 3 \cdot 7 \cdot 8$$

$$42 = 2 \cdot 3 \cdot 7$$

$$d(a.b,42)=1$$

هذا يعني أن a مع 3 ، 7 و 8

$$d(a,3)=d(a,7)=d(a,8)=1$$

$$d(b,3)=d(b,7)=d(b,8)=1$$

$$a^{2} \equiv 1 \pmod{3}$$

$$a^{6} \equiv 1 \pmod{7}$$

وبالتالي لا نكتب

$a^{7} \equiv 1 \pmod{8}$ لأن 8 ليس عدد أولي ولا ينطبق

/ /

عليها مبرهنة جزئيا.

$d(a.b, 8)=1$

a.b لا يمكن ان يكونا زوجيين ولا يمكن احدهما فردي والآخر زوجي
وبالتالي a و b عددان فرديان

$a^2 \equiv 1 \pmod 8$

$b^2 \equiv 1 \pmod 8$

$\Rightarrow a^6 \equiv 1 \pmod 8$ } بالطرح حسب خواص
$b^6 \equiv 1 \pmod 8$ } التطابقات

$(a^6 - b^6) \equiv 0 \pmod 8$

$\Rightarrow 8 \mid (a^6 - b^6)$

وبالتالي جاد 8.7.3 تقسم $(a^6 - b^6)$

* مبرهنة ولسن ساب الهيثم:
اذا كان P عددا أوليا فإنه ؛

$$(P-1)! \equiv -1 \pmod P$$

$\mathbb{Z}_p$ in $(P-1) + \boxed{1} = 0$

$(-1) = P-1$

or $P \mid [(P-1)! + 1]$

or

$(P-1)! \equiv (P-1) \pmod P$

$(P-1)(P-2)! \equiv (P-1) \pmod P$

بما ان $(P-1)$ اولي مع العدد الاولي P وبالتالي يمكن الاختصار عليه

$$(P-2)! \equiv 1 \pmod P$$

عكس مبرهنة ولسن صحيح

/ /

البرهان: عندما $p=2$ محققة $\quad 1 \equiv -1 \pmod{3}$

عندما $p=3$ $\quad 2 \equiv -1 \pmod{3}$

نفرض أن $p>3$

لو أخذنا المجموعة

$p-1$ هو (-1)

$$A = \mathbb{Z}_p \setminus \{\bar{0}, \pm\bar{1}\}$$

$$A = \{2, 3, \dots, p-2\}$$

$|A| = p-3$ رتبة المجموعة

عدد p أولي وبالتالي طرحه من 3 هو عدد زوجي

$a \in A \;:\; d(a,p)=1$

$\exists\, a^* \in A \;;\; a \cdot a^* \equiv 1 \pmod{p}$

معكوس (1) هو (1) $\quad$ معكوس $p-1$ هو (-1)

$a^* \not\equiv a \pmod{p}$

لو أخذنا المثال التالي

$p=13$

$A = \{2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

$4 \cdot (10) \equiv 1 \pmod{13}$

$(4^{-1}) = 10$

عندئذ تتوزع a إلى $\left(\frac{p-3}{2}\right)$ زوج بحيث حاصل ضرب أي زوجين مترافقين يطابق 1 بالمقياس p وبالتالي في المثال:

$2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \equiv 1 \pmod{13}$

$2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p}$

نضرب طرفي التطابق

$2 \cdot 3 \cdots (p-2)(p-1) \equiv (p-1) \pmod{p}$

$(p-1)! \equiv -1 \pmod{p}$

عكس مبرهنة ولسن :

إذا كان $n \geq 2$ ، $(n-1)! \equiv -1 \pmod{n}$

فعندئذ n يكون أولي .

البرهان :

إذا لم يكن n أولياً وبالتالي هو عدد مؤلف أي له قاسم مثل d بحيث

$d \mid n$ حيث $1 < d < n$

أي $1 < d \leq n-1$ وهذا ينتج $d \mid (n-1)!$ ——— (1)

من جهة أخرى :

من الفرض n ، $n \mid (n-1)! + 1$

وبالتالي $d \mid ((n-1)! + 1)$ ——— (2)

من العلاقتين (1) و (2)

$$d \mid \{(n-1)! + 1 - (n-1)!\} = 1$$

وبالتالي $d = 1$ وهذا يناقض مع كون n ليس أولياً

وبالتالي n أولي .

ملاحظة :

يمكن صياغة مبرهنة ولسن وعكسها على النحو الآتي :

يكون $1 < n \in \mathbb{Z}$ أولياً إذا وفقط إذا كان

$$(n-1)! \equiv -1 \pmod{n}$$

ولكن هذا المعيار للأعداد الأولية صعب بسبب سرعة تزايد $n!$ وخاصة عندما يكون n عدداً كبيراً .

تمرين :

أثبت أن

$$18! \equiv -1 \pmod{437}$$

$$(20)^2 < 437 < (21)^2$$

$$(21)^2 - 437 = 4$$

$$437 = 19 \cdot 23$$

اثبت ان العدد

$$127 \mid [7 \cdot (125)! + 5!]$$

127 عدد اولي حسب ويلسن

$$(126)! \equiv -1 \pmod{127}$$

$$126 \cdot (125)! \equiv -1 \pmod{127}$$

$$(-1)(125)! \equiv -1 \pmod{127}$$

$$(125)! \equiv 1 \pmod{127}$$

$$7 \cdot (125)! \equiv 7 \pmod{127}$$

نضيف للطرفين $5!$

$$5! + 7 \cdot (125)! \equiv 7 + 5! \pmod{127}$$

$$\equiv 127 \pmod{127}$$

$$5! + 7 \cdot (125)! \equiv 0 \pmod{127}$$

وبالتالي

$$127 \mid [7(125)! + 5!]$$

هذا الجزء أكثر تطبيقات على مبرهنة [illegible] ومبرهنة [illegible] والمبرهنة [illegible]

مبرهنة:

إذا كان P عدداً أولياً فردياً فإن للتطابق

$$x^2 \equiv -1 \pmod{P}$$

حل إذا وفقط إذا كان

$$P \equiv 1 \pmod{4}$$

وإذا كان ذلك كذلك

$$P \equiv 1 \pmod{4}$$

فإن

$x = \left(\frac{P-1}{2}\right)!$ حل للتطابق

$$x^2 \equiv -1 \pmod{p}$$

مثال:

إذا كان $p=5$ حيث $5 \equiv -1 \pmod{4}$

$$x = \left(\frac{5-1}{2}\right)! = 2! = 2$$

$$(2)^2 = 4 \equiv -1 \pmod{5}$$

$p = 13$

$$x = \left(\frac{13-1}{2}\right)! = 6! = 720$$

$$(720)^2 \equiv \quad \pmod{13}$$

* * *

تم بحمد الله